KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

BEFORE THE FEDERAL COMMUNICATIONS COMMISSION

IN THE MATTER OF

COMMENTS SOUGHT ON PRIVACY AND SECURITY OF INFORMATION STORED ON MOBILE COMMUNICATIONS DEVICES

CC Docket No. 96-115

JULY 13, 2012

The Center for Democracy & Technology ("CDT") submits these comments in response to the Commission's Public Notice regarding privacy and security of information stored on mobile communications devices. CDT is a nonprofit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the decentralized Internet.

We applaud the Commission's continuing examination of privacy and security concerns presented by the increasing collection of data on mobile devices, and appreciate the opportunity to address how to best protect consumer interests as these devices become an increasingly important presence in our society.

We highlight the privacy risks created by collection of data via mobile devices, and emphasize that shifts in mobile usage are diminishing the impact of existing telecommunications-based privacy rules. While the CPNI rules could possibly be read to apply to some forms of information acquired by software that is identical to personal information carriers already obtain, it cannot be read to apply to information not otherwise available to carriers such as HTTPS encrypted web browsing activities. Certainly, under no reasonable interpretation could the CPNI rules be construed to offer comprehensive privacy protections for mobile users. For this reason, CDT urges the Commission to call for comprehensive privacy rules based on the Fair Information Practice Principle to fully protect consumers during this time of rapidly evolving mobile computing.

I. Collection of Data Through Mobile Devices Significantly Threatens User Privacy

The rapid development of smartphones has provided a multitude of benefits to users, but has also created unprecedented risks to privacy. The range of personal data available through devices, and the vast number of applications and software on smartphones that can collect these data, put users' private information at risk of exposure. According to one recent report, over 80 million

apps have been downloaded that contain "aggressive" ad networks which data-mine sensitive information such as users' email addresses, phone numbers, and location data.[1] Popular apps have been revealed to record users address books[2] and calendars,[3] and 47 of the 101 most popular mobile apps transmit users' locations off the device.[4]

Potential exposure and misuse of these data creates serious risks for users. Location information can be abused by stalkers and perpetrators of domestic violence.[5] Disclosure of web activity, contact lists, and communication histories leave individuals vulnerable to targeted hacking schemes. And location data, web browsing activities, and search queries can reveal sensitive personal information such as medical issues, sexual orientation, religious beliefs, and political affiliation. Consumers who do not trust the mobile ecosystem to protect their privacy may be deterred from fully taking advantage of these devices or from using them for potentially sensitive purposes.[6]

By and large, consumers today do have the sufficient information and tools to exercise control over the retention, use, and transfer of personal information generated by their mobile devices. According to a recent study conducted by researchers at the Berkeley Center for Law & Technology, "Americans overwhelmingly consider information stored on their phones to be private."[7] Despite this belief, users' ability to address this issue is highly limited. Researchers at Carnegie Mellon University concluded that an average consumer would need to spend between 181 and 304 hours each year reading Web site privacy policies to reach a basic understanding of how his or her information is being collected and used.[8] And over 80

---

[1] Reuters, *Privacy risk from ads in apps rising -security firm* (July 9, 2012), *available at* http://in.reuters.com/article/2012/07/09/mobile-advertising-idINL6E8I83R720120709.

[2] Hayley Tsukayama, The Washington Post, *Path app under fire for copying address books* (February 8, 2012), *available at* http://www.washingtonpost.com/business/technology/path-app-under-fire-for-copying-address-books/2012/02/08/gIQArNFCzQ_story.html.

[3] Adrian Kingsley-Hughes, Forbes, *LinkedIn iOS App Grabs Names, Emails And Notes From Your Calendar* (June 6, 2012), *available at* http://www.forbes.com/sites/adriankingsleyhughes/2012/06/06/linkedin-ios-app-grabs-names-emails-and-notes-from-your-calendar/.

[4] Scott Thurm and Yukari Iwatani Kane, The Wall Street Journal, *Your Apps are Watching You* (December 17, 2010), *available at* http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

[5] See, e.g., Rob Stafford, Tracing a Stalker, *Dateline NBC* (June 16, 2007), *available at* http://www.msnbc.msn.com/id/19253352/. See also, Ben Goldacre, The Guardian, *How I stalked my girlfriend* (January 31, 2006), *available at* http://www.guardian.co.uk/technology/2006/feb/01/news.g2.

[6] Don Davis, *Consumer privacy fears limit the growth of m-commerce, Forrester says*, Internet Retailer, June 17, 2011, http://www.internetretailer.com/2011/06/17/barriers-mobile-commerce-growth.

[7] Urban, Jennifer M., Hoofnagle, Chris Jay and Li, Su, Mobile Phones and Privacy (July 10, 2012). BCLT Research Paper Series. Available at SSRN: http://ssrn.com/abstract=2103405.

[8] Aleecia McDonald and Lorrie Faith Cranor, *The Cost of Reading Privacy Policies, I/S: A Journal of Law and Policy for the Information Society* (2008 Privacy Year in Review issue), *available at* http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf.

percent of the 340 most popular free mobile apps do not contain a privacy policy at all.[9] Studies of ordinary users trying to interact with privacy tools show that they cannot meaningfully control the distribution of their personal information.[10] With users unable to understand and control how their data are being collected, they are exposed to potential abuse by entities obtaining their private information.

II. Consumer Use of Mobile Devices is Migrating Beyond the Reach of Existing Telecommunications Rules

Consumer use of smartphones is increasing dramatically. Over the past two years, smartphone ownership has risen by 18 percent.[11] This year, for the first time ever, a majority of Americans now use a smartphone.[12] As technological advances push prices ever lower while expanding availability, usage is likely to continue to grow.

Previously voice-based devices, smartphones are now powerful personal computers. Phone calls, once the central feature of mobile devices, are increasingly cast as a secondary function. Internet browsing and a wide variety of web-based apps play a key role in smartphone activity, and their use is rapidly increasing. In 2011, data usage on mobile devices tripled.[13] The majority of Internet traffic now occurs on mobile devices, rather than on laptop and desktop computers.[14] And 25 percent of smartphone owners say that they primarily use their phones rather than computers to access the Internet.[15]

Carriers are recognizing the decreasing relative importance of voice calls and increasing centrality of data services. Recently, Verizon announced its intention to exclusively offer data-centric pricing plans with unlimited voice and texting as auxiliary features.[16] AT&T has also expressed interest in such a shift, converting voice calls and texts to a component of

---

[9] Mark Hachman, PC Magazine, *Most Mobile Apps Lack Privacy Policies: Study* (April 27, 2011), *available at* http://www.pcmag.com/article2/0,2817,2384363,00.asp.

[10] Peter Leon *et al.*, *Why Johnny Can't Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*, Carnegie Mellon University Technical Report, October 31, 2011, http://www.cylab.cmu.edu/research/techreports/2011/tr_cylab11017.html.

[11] Leslie Horn, PC Mag, *U.S. Smartphone Use on the Rise, With Android Leading the Charge* (December 15, 2011), available at http://www.pcmag.com/article2/0,2817,2397688,00.asp.

[12] Chris Burns, Slash Gear, *Nielsen: first time Smartphone and Feature Phone usage equal* (March 30, 2012), *available at* http://www.slashgear.com/nielsen-first-time-smartphone-and-feature-phone-usage-equal-30220760/.

[13] Cisco, *Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2011–2016* (February 14, 2012), *available at* http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.

[14] *Id*.

[15] Aaron Smith, Pew Internet, *Smartphone Adoption and Use* (July 11, 2011), available at http://pewinternet.org/Reports/2011/Smartphones.aspx.

[16] Techland, *Verizon to Ditch Phone Plans in Favor of Shared Data Plans* (June 12, 2012), *available at* http://techland.time.com/2012/06/12/verizon-to-ditch-phone-plans-in-favor-of-shared-data-plans/.

data usage.[17] With cost for calls and text messaging based only on data usage, carriers will be less incentivized to compete with third-party applications that provide new and innovative versions of those communications services.[18] And as Wi-Fi penetration continues to increase,[19] carriers may often be completely uninvolved in these app-based communications occurring on smartphones.

Mobile broadband services are today classified as "information services" under Title I.[20] As a result, the CPNI rules' patchwork application to mobile devices is becoming increasingly tenuous as usage patterns shift away from "telecommunications services" as currently understood. While it is important for the Commission to apply the CPNI rules to their full effect, they are themselves sorely insufficient to protect consumers' privacy in today's mobile landscape.[21]

CDT encourages the FCC to vigorously protect consumer privacy within the limits of statutory authority.

III. The CPNI Rules Provide Incomplete Protections

The Telecommunications Act of 1996 defined and established protections for CPNI, sensitive data collected by telecommunication companies regarding their customers' communications. This information consists of "quantity, technical configuration, type, destination, location, and amount of use" of telecommunication services.[22] Further, in order for information to qualify as CPNI, it must be "*made available to the carrier by the customer solely by virtue of the carrier-customer relationship*."[23] It is this limiting feature that makes application of CPNI protections to data acquired by software such as Carrier IQ difficult.

---

[17] Under this plan, "phone calls and texts would be considered as just another form of data." The Wall Street Journal, *AT&T: Data-only plans coming for phones in 2 years* (June 1, 2012), *available at* http://online.wsj.com/article/AP27b164dd4bfa43a882ce8fb2a137a81c.html.

[18] For example, iMessage, a texting application for iPhones, contains several features not available through SMS texting. David Pogue, The New York Times, *The Disruptive Power of iMessage* (March 22, 2012), *available at* http://pogue.blogs.nytimes.com/2012/03/22/the-disruptive-power-of-imessage/.

iMessage already has 140 million users. Terrance O'Brien, Engadget, *Apple brags: sells 365 million iOS devices, 140 million iMessage users* (June 11, 2012), *available at* http://www.engadget.com/2012/06/11/apple-brags-sells-365-million-ios-devices-140-million-imessage/.

New platforms have already begun competing to develop a dominant role in the mobile messaging market. Josh Constine, Tech Crunch, *The Apple / Google / Facebook Message War Starts Now* (July 2, 2012), *available at* http://techcrunch.com/2012/07/02/message-war/.

[19] The United States currently has 61 percent Wi-Fi penetration. Frederic Lardinois, Tech Crunch, *Study: 61% of U.S. Households Now Have WiFi* (April 5, 2012), *available at* http://techcrunch.com/2012/04/05/study-61-of-u-s-households-now-have-wifi/.

[20] *See Nat'l Cable & Telecommunications Ass'n v. Brand X Internet Services*, 545 U.S. 967 (2005).

[21] Testimony of Justin Brookman, Director of Consumer Privacy, Center for Democracy & Technology before the Senate Judiciary Subcommittee on Privacy, Technology, and the Law Hearing on "Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy," May 10, 2011, https://www.cdt.org/files/pdfs/20110510_mobile_privacy.pdf.

[22] 47 U.S.C. 222(h)(1)(A).

[23] Id.

On one hand, carriers play a significant role in placing monitoring software on smartphones, and the data collected by monitoring software is almost precisely the same data as the carrier could obtain "solely by virtue of the carrier-customer relationship." On the other hand, the Carrier IQ software had capabilities that clearly extended beyond what traditional carrier networks can do. Even in the simplest cases, the CPNI rules' application to monitoring software remains uncertain.

A. The CPNI rules could potentially be read to provide consumers with limited protections regarding monitoring software placed on their smartphones.

Carriers are able to use their role in the output and sale of smartphones to ensure that software such as Carrier IQ is installed on devices before they are sold to or used by consumer. Manufacturer installation only occurs because of contractual obligations required by the carriers.[24] As a result, consumers have no knowledge of the software's presence, or ability to choose whether it remains on their devices. Google has stated that due to this early installation of the software, it is unable to block or remove it from Android devices.[25]

A significant portion of the data acquired by Carrier IQ are identical to the communications information that carriers already receive in a manner that entitles it to CPNI protection. For example, Sprint states, "As a wireless service provider, Sprint knows the location of devices registered on its network *irrespective of Carrier IQ diagnostics*."[26] Sprint and AT&T make similar claims regarding other types of data acquired by Carrier IQ.[27,28]

---

[24] According to Samsung, "Pursuant to the carriers' agreements with [Samsung], some of those cellular carriers required Samsung to pre-install Carrier IQ software on some of the devices prior to the sale of those devices to the carrier (and before the sale of the devices to the consumer by the distributor, carrier or its agent)." Dale Sohn, *Letter from Samsung Telecommunications America to Senator Al Franken* (December 14, 2011), *available at* http://www.franken.senate.gov/files/letter/111214_Samsung_Response_to_Sen_Franken_CarrierIQ.pdf.

HTC similarly states, "This integration [of Carrier IQ software] is required by the wireless service providers and performed under contract and per their specifications." Peter Chou, *Letter from HTC Corporation to Senator Al Franken* (December 14, 2011), *available at* http://www.franken.senate.gov/files/letter/111214_HTC_Response_to_Sen_Franken_CarrierIQ.pdf.

[25] According to Google, "Android is an open source effort and we do not control how carriers or OEMs customize their devices." Dieter Bohn, The Verge, *Google confirms: we have no 'affiliation with Carrier IQ'* (December 1, 2012), *available at* http://www.theverge.com/2011/12/1/2604060/google-confirms-no-affiliation-carrier-iq/in/2365736.

[26] Vonya McCann, *Sprint Response Letter to Senator Al Franken* (December 14, 2011), *available at* http://www.franken.senate.gov/files/letter/111214_Sprint_Response_to_Sen_Franken_CarrierIQ.pdf (emphasis added).

[27] Id ("We know the cell site on which a phone is registering its location, which is necessary for the delivery of voice and data services. We also know the telephone numbers to which our customers have initiated a call or sent a text. Such data is necessary to deliver telecommunications services. In many cases the data collection is required by law and regulations. Under federal law, Customer Proprietary Network Information (CPNI) is also privacy protected.").

[28] Tim McKone, AT&T Response Letter to Senator Al Franken (December 14, 2011), *available at* http://www.franken.senate.gov/files/letter/111214_Att_Response_to_Sen_Franken_CarrierIQ.pdf ("As a network service provider, we have access to a great deal of information necessarily incident to the provision of service.").

Given the role of carriers in ensuring the installation of software such as Carrier IQ and the nature of the data acquired, CPNI protections reasonably could be applied to some of the personal data acquired by software that are identical to the data acquired by carriers as a result of providing communications services.

The Commission could in these instances require carriers to notify subscribers that such data collection software is in use on their device. In addressing pretexting in 2007, the Commission expressed concern regarding unauthorized disclosure of CPNI, including through means unanticipated at the time.[29] The Commission's basis for requiring customer notification of unauthorized disclosure supports regulation of software such as Carrier IQ. The Commission stated, "By mandating the notification process adopted here, we better empower consumers to make informed decisions about service providers."[30] The discovery of Carrier IQ on smartphones quickly became a major news story, generating significant controversy and provoking anger among consumers. Carriers and manufacturers who refused to install the software highlighted their decision, while many companies who utilized the software quickly qualified or discontinued their use of it.[31] Clearly notification by carrier regarding use of such software would "better empower consumers to make informed decisions about service providers," fulfilling the Commission's previously stated goal.

If the Commission does extend CPNI protections to personal data acquired by software such as Carrier IQ, it should consider adopting new rules requiring that data be stored locally in a form that cannot be read or deciphered without a key. Carrier IQ stores data on devices, making the data a valuable target for hackers before ever being transferred to carriers.[32] Furthermore, encryption (or a similar technology) could protect against unrestricted law enforcement access to this information, a practice that may currently be occurring.[33] The Commission has previously considered implementation of mandatory encryption rules for CPNI,[34] though we would caution the Commission against mandating any particular technological approach. The technological advances that have occurred in recent years and risks posed to smartphone users by leaving unencrypted data on devices make such a measure worthy of renewed consideration.

---

[29] Report and Order and Further Proposed Rulemaking, FCC, CC Docket No. 96-115 (April 2, 2007), at 20 ("[W]e recognize that numerous types of circumstances – including situations other than pretexting – could result in the unauthorized disclosure of a customer's CPNI to a third party.").

[30] Id, at 19.

[31] Brad Molen, Engadget, *Which companies are on the Carrier IQ bandwagon?* (December 1, 2011), *available at* http://www.engadget.com/update/carrier-iq-which-companies-have-the-smarts; Christina DesMarais, PC World, *Sprint's Decision to Stop Using Carrier IQ a Win for Privacy Advocates* (December 17, 2011), *available at* http://www.pcworld.com/article/246497/sprints_decision_to_stop_using_carrier_iq_a_win_for_privacy_advocates.html.

[32] According to former FTC staff technologist Christopher Soghoian "This would be a gold mine for a hacker." David Goldman, CNN, *Carrier IQ: Your phone's secret recording device* (December 1, 2011), *available at* http://money.cnn.com/2011/12/01/technology/carrier_iq/index.htm.

[33] *See* Tom Loftus, The Wall Street Journal, *Carrier IQ Fights Speculation Around FBI Link* (December 13, 2011), *available at* http://blogs.wsj.com/digits/2011/12/13/carrier-iq-fights-speculation-around-fbi-link/?mod=WSJBlog&mod.

[34] Report and Order and Further Proposed Rulemaking, FCC, CC Docket No. 96-115 (April 2, 2007), at 21.

B. The CPNI rules are subject to clear limitations which complicate their application.

While the prior interpretation would benefit consumers and can (for some data) be consistently read within the spirit of the CPNI rules, the limitations of the CPNI rules cannot be ignored. Much — and quite possibly all — of the data acquired by Carrier IQ are not "made available to the carrier by the customer *solely by virtue of the carrier-customer relationship*,"[35] and therefore might not be protected by the CPNI rules at all.

First, some sorts of data collection are clearly outside of the scope of the CPNI rules. For example, certain web browsing activities recorded by Carrier IQ — notably HTTPS encrypted web browsing and search engines queries — are not normally available to carriers.[36] Further, Carrier IQ provides information regarding communications in a far more precise form than is ever available to carriers as a result of the carrier-customer relationship.[37] Finally, when smartphones are operating over Wi-Fi networks, information regarding web-based activity on the devices is not regularly available to carriers but can be obtained through Carrier IQ.[38] The ability of carriers to obtain these data is in no way linked to their role as carriers, or duplicative of data that are acquired as a result of the carrier-customer relationship. Therefore they cannot be categorized as CPNI.

Second, there is an argument that even data acquired by Carrier IQ identical to those independently acquired by carriers as a result of the carrier-customer relationship should not qualify as CPNI. Due to the refusal of some manufacturers to install Carrier IQ, the data it

---

[35] 47 U.S.C. 222(h)(1)(A) (emphasis added).

[36] According to former FTC staff technologist Ashkan Soltani, "In no case would [carriers] normally get access to secure HTTPs browsing activity." Ashkan Soltani, *Overlogging – It's Not Just About Trees*, *available at* http://ashkansoltani.org/docs/carrier_IQ.html.

See also Christopher Sogohian, slight paranoia, *Sprint recklessly exposed Carrier IQ logged URL data to easy government access* (December 19, 2011), *available at* http://paranoia.dubfire.net/2011/12/sprint-recklessly-exposed-carrier-iq.html ("Sprint falsely denies collecting users' search query information (the search terms are in the Google/Bing URL) . . . Sprint collects through Carrier IQ the URLs of webpages viewed over encrypted HTTPS connections which it would never learn by watching the network.").

[37] *See* Vonya McCann, *Sprint Response Letter to Senator Al Franken* (December 14, 2011), *available at* http://www.franken.senate.gov/files/letter/111214_Sprint_Response_to_Sen_Franken_CarrierIQ.pdf ("There are some things that Sprint does not know. Sprint does not always know why a call drops or a website will not load, for example. Sprint may not always know why a text message is not delivered timely, or why service is unavailable in a particular area.").

See also Tim McKone, *AT&T Response Letter to Senator Al Franken* (December 14, 2011), *available at* http://www.franken.senate.gov/files/letter/111214_Att_Response_to_Sen_Franken_CarrierIQ.pdf ("[Carrier IQ] provides us with a device-side view of the customer's experience – a view that cannot be obtained from the network alone.").

[38] *See* Ashkan Soltani, *Overlogging – It's Not Just About Trees*, *available at* http://ashkansoltani.org/docs/carrier_IQ.html ("While your carrier has access to location (via cell towers) and non-HTTPS browsing history on account of providing you wireless service, they typically do not receive this information when you're using your home WiFi.").

See also Christopher Sogohian, slight paranoia, *Sprint recklessly exposed Carrier IQ logged URL data to easy government access* (December 19, 2011), *available at* http://paranoia.dubfire.net/2011/12/sprint-recklessly-exposed-carrier-iq.html ("[Sprint] probably also gets through Carrier IQ the URLs accessed by handset owners when they are using WiFI and not Sprint's network.").

acquires cannot be obtained by carriers from a significant number of smartphones.[39] Carriers are similarly restricted by closed operating systems that do not install the software.[40] Furthermore, as recent incidents demonstrate, other entities such as smartphones apps are capable of acquiring similar information in the same manner as Carrier IQ.[41] The inability of carriers to acquire data through Carrier IQ on a substantial number of smartphones, and the ability of non-carriers to acquire data through similar software, diminishes the argument that the data Carrier IQ obtains is made available "solely by virtue of the carrier-customer relationship," and can therefore be categorized as CPNI.

IV. A Need for Comprehensive Privacy Rules

Even if CPNI protections are read to cover limited sorts of data collection from monitoring software such as Carrier IQ, they cannot fully apply to all data collection and use that occurs.[42] And as use of smartphones becomes more data driven and centered upon mobile computing, a greater portion of smartphone activities — and potentially even those activities traditionally covered such as calls and texts — will fall outside the bounds of CPNI protection.[43] Given the inability of existing law to adequately protect consumers now and in the future, we urge the Commission to join the White House[44] and the Federal Trade Commission[45] in calling for new legislation which sets a baseline for the conditions under which consumer data of all types can be collected and used.

The Fair Information Practices (FIPPs) should be the foundation of any comprehensive privacy framework. FIPPs have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and other sectoral federal privacy laws that govern commercial uses of

---

[39] RIM, HP, Nokia have stated that they refuse to install Carrier IQ for carriers. Catherine Smith and Jason Gilbert, The Huffington Post, *Carrier IQ: Verizon, Apple, Google, Microsoft, AT&T And Others Speak Out On Phone 'Tracking' Controversy* (December 2, 2011), *available at* http://www.huffingtonpost.com/2011/12/01/carrier-iq-verizon-apple-google-microsoft-att_n_1124779.html#s513592&title=HP. Brad Molen, Engadget, *Which companies are on the Carrier IQ bandwagon?* (December 1, 2011), *available at* http://www.engadget.com/update/carrier-iq-which-companies-have-the-smarts.

[40] John Paczkowski, All Things D, *Apple: We Stopped Supporting Carrier IQ With iOS 5* (December 1, 2011), *available at* http://allthingsd.com/20111201/apple-we-stopped-supporting-carrieriq-with-ios-5/?mod=tweet.

[41] *See* Hayley Tsukayama, The Washington Post, *Path app under fire for copying address books* (February 8, 2012), *available at* http://www.washingtonpost.com/business/technology/path-app-under-fire-for-copying-address-books/2012/02/08/gIQArNFCzQ_story.html.

See also Adrian Kingsley-Hughes, Forbes, *LinkedIn iOS App Grabs Names, Emails And Notes From Your Calendar* (June 6, 2012), *available at* http://www.forbes.com/sites/adriankingsleyhughes/2012/06/06/linkedin-ios-app-grabs-names-emails-and-notes-from-your-calendar/.

[42] *See supra*, Section III.B.

[43] *See supra*, Section II.

[44] The White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, Report, February 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[45] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers, Report, March 2012, http://ftc.gov/os/2012/03/120326privacyreport.pdf.

information online and offline. The formulation of the FIPPs by the Department of Homeland Security offers a robust set of modernized principles that should serve as the foundation for any discussion of consumer privacy legislation.[46] Those principles are:

- Transparency
- Purpose Specification
- Use Limitation
- Data Minimization
- Data Accuracy
- Individual Participation
- Security
- Accountability

For particularly sensitive data, such as health information, financial information, information about religion or sexuality, and — most relevant here — precise geolocation data, a legislative framework should provide for enhanced application of the Fair Information Practice Principles, including for affirmative opt-in consent for the collection and/or transfer of such information. Consumers understandably have greater concerns about the use and storage of such information, and the law should err against presuming a consumer's assent to share such information with others.

Technological advances in the use of smartphones additionally reflect the need to reform policy regulating law enforcement acquisition of private data. While it appears likely that law enforcement obtained data from Carrier IQ, little is known regarding how this occurred or whether any judicial oversight existed.[47] Carrier IQ, and similar software programs, have the potential to collect a wide range of personal information. The legal standards regulating law enforcement acquisition of some of these data are ambiguous due to the outdated nature of the Electronic Communications Privacy Act (ECPA), leaving businesses unsure of their respective obligations to customers and the government. In other instances, such as with geolocation information, existing legislation provides no regulation of government acquisition of data. In advocating for enhanced protection for smartphone users, the Commission should also support comprehensive protection of personal data from unreasonable government access absent proper judicial oversight.

[46] U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, December 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.
[47] *See supra*, Section III.B.